Identifying Security Threats and Privacy Challenges in Social Networks

Simeon Ayoade Adedokun

A Term Paper Presented at the Department of Computer Science, Ladoke Akintola University of Technology, Ogbomoso

November 2023

Abstract

Security and privacy on social networks have become increasingly important as these platforms continue to gain popularity. This paper explores the measures and policies implemented to protect users' personal information and ensure their online safety. It discusses the importance of security and privacy in social networks and computational strategies to address potential attacks. The paper also provides insights into the strengths and weaknesses of existing security measures, and identification of emerging security threats and challenges, in order to help researchers and developers develop more effective strategies to improve the security and privacy of social networks. It emphasizes the need for users to exercise caution in sharing personal information and regularly review and update their privacy settings. The paper emphasizes the importance of maintaining a secure and private online presence on social networks.

Keywords*: social, network, security, privacy, phishing, anonymity, identity*

1. Introduction

A social network is an online platform or service that allows individuals to connect, communicate, and interact with others. These platforms typically enable users to create a profile, share information, and engage with others through various features such as posting updates, sharing photos or videos, messaging, commenting, and liking. Social networks can be general-purpose platforms like Facebook, Twitter, and Instagram, which cater to a wide range of users and interests.

A social network refers to the connections between entities, often individuals, through personal relationships, interactions, and information flow. Social networks facilitate social interactions and enable users to connect with friends, family, colleagues, and even strangers. They provide a space for sharing thoughts, experiences, and media, as well as staying updated on the activities and lives of others. In a broader sense, a social network refers to a structure that represents the relationships and connections between entities, which can include individuals, organizations, or even concepts. These connections can be based on various factors such as personal relationships, professional connections, shared interests, or common affiliations. In the context of social media platforms, the term "social network" is often used

to describe the online platforms or services that facilitate these connections and interactions between individuals. These platforms provide a digital representation of social networks by allowing users to create profiles, connect with others, and share information and content (Joshi & Kuo, 2011).

The concept of social networks extends beyond just individuals and personal relationships. It can also be applied to other domains such as business networks, academic networks, or even networks of ideas and concepts. There are niche social networks that focus on specific interests or communities, such as LinkedIn for professional networking or Pinterest for sharing and discovering visual content. In these cases, the connections between entities represent professional collaborations, academic collaborations, or the flow of information and influence.

Whatever the objective of a social network, the ability to share information and facilitate social interactions amongst users is one of the primary reasons people sign up, create a profile, and utilize the various applications available on the network. Sharing or disclosing personal information on social networks is a double-edged sword that can be both beneficial and harmful (Chen & Yang, 2008). On one side, exposure of personal information is typically essential and advantageous for those who wish to engage in social communities online. Creating public friend lists and making user profiles visible are essential for implementing the basic features of social networks, like social search. However, personal information exposure—especially one's identity—can lead to malicious attacks from both the real world and the internet, including phishing, reputation slander, customized spamming, and stalking (Acquisti et al., 2007).

These platforms have become an integral part of modern communication and have transformed the way people interact and share information. Social networks can be seen as a way to understand and visualize the relationships and interactions that exist between entities, whether they are individuals, organizations, or ideas. However, it is important to be mindful of security and privacy considerations when using social networks, as they can involve sharing personal information and interacting with a wide range of individuals. More effective and flexible security mechanisms are needed for user safety and the continued success of social networks (Mattioli et al., 2023).

This paper is aimed at identifying security threats and privacy challenges in social networks. In this paper, the importance of security and privacy in social networks and computational strategies to address potential attacks are discussed. The paper also discusses various aspects of security and privacy, such as different attack strategies that an attacker may use, security techniques to prevent these attacks, and metrics to measure the effectiveness of these techniques. The paper also provides insights into the strengths and weaknesses of existing security measures, and identification of emerging security threats and challenges, in order to help researchers and developers develop more effective strategies to improve the security and privacy of social networks.

2. Features of Social Networks

The aim and motivation of this paper is to discuss the desirable features and possible implementations of social networks without and provide insight into different strategies to enhance privacy and security in social networks. Being online platforms that enable individuals to connect, communicate, and share information with others, the main functionalities of social networks can vary depending on the platform, but they share some common features. According to Boyd & Ellison (2007); Kenton (2023); Naseer (2023); Zhang et al. (2010), social networks as digital representations of their users, have the following characteristics:

1. Enable users (individuals and businesses) to create digital representations of themselves (i.e. *user profiles*), and express their connections with other users or businesses.
2. Encourage users in the real or virtual world to maintain and strengthen their current social connections.
3. Assist in establishing new relationships based on shared hobbies, interests, locations, and so on.

Based on the above recommendations, a social network should provide the following functionalities in order to fulfill its purpose of allowing individuals to have their digital representations, connect, communicate, and interact with one another regardless of their location, interests, or backgrounds.

(i) **Profile Creation and Management**

A social network typically allow creation and management of personal space—allowing every user to set up and maintain an online presence. A user should be able to:

- Create and delete personal account.
- Create and edit personal profile, and provide information about themselves, such as their name, profile picture, bio, and interests.
- Upload and edit personalized generated contents based on certain allowed rules.

(ii) **Connection with Others**

Connection with others on social networks refers to the process of building relationships, engaging with people, and creating a sense of community on social media platforms. Social networks provide formal powerful tools for individuals, brands, and organizations to connect with others, share information, and build relationships. Users can connect with friends, family, colleagues, or other individuals by sending friend requests, following their profiles, or accepting connection requests. This allows users to build a network of contacts and stay updated on their activities.

(iii) **Sharing Information**

Social networks provide means of communication that allows users to exchange of information, ideas, and messages between individuals, brands, or organizations on social media platforms. It

involves various forms of communication, such as posting updates, commenting, direct messaging, and engaging in discussions. Some key aspects of communication on social networks include posting updates, commenting and engaging, direct messaging, harshtags and mentions, livestreaming, sharing and resharing, polls and surveys, emojis and visual communication, influencer collaboration, and crisis management.

Social networks usually have a central feed or timeline where users can see updates from their friends or connections. This feed is typically personalized based on the user's preferences and activities.

To ensure effective communication and timely responses, social networks send notifications to users to alert them about new friend requests, messages, comments, likes, or other relevant activities happening within their network.

(iv) **Groups and Communities**

Groups and communities on social networks are online spaces where individuals with shared interests, hobbies, goals, or affiliations come together to connect, engage, and share content, and engage in discussions. These groups and communities can be found on various social media platforms, such as Facebook, LinkedIn, Reddit, or even niche-specific platforms. These groups and communities provide a platform for like-minded people to interact, collaborate, and support each other. Some key aspects of groups and commuities on social networks are purpose and interests, membership and access, discussions and engagement, content sharing, networking and collaboration, events and meetups, group rules and moderation, expertise and learning opportunities, privacy and security.

(v) **Exploring and Discovering in the Digital Social Space**

Exploring the digital social space involves discovering and engaging with various aspects of the online community. Social networks do more than interaction, encouraging users to establish new connections, and information sharing. They provide support for searching or traversing the digital social space, which is a crucial component of social networks that allow users to browse a new user's personal space, whether through the means of social search or social traversal. Social networks often have features that allow users to discover new connections, discover new content or curated content based on their interests, explore trending topics, attend virtual events, participate in challenges and campaigns, and more (Fong et al., 2009; Patil & Shyamasundar, 2017).

(vi) **Analytics and Insights**

Social networks often offer analytics tools for users with business or professional profiles. Analytics and insights on social networks provide valuable data and information about a brand's social media performance, audience demographics, engagement metrics, and content effectiveness. These analytics help users understand how their social media efforts are performing, identify areas for improvement, and make data-driven decisions to optimize your social media strategy. These tools provide insights into the performance of their posts, audience demographics, and engagement metrics (Ayodeji & Kumar, 2019).

The functionalities of social networks can evolve and change over time as platforms introduce new features and adapt to user needs and preferences.

4. Security Threats on Social Networks

Social media provides a platform for people to interact and exchange videos, images, and personal stories. However, excessive sharing or failing to recognize imposters might endanger personal and commercial accounts.

Social media accounts are frequently used by attackers during the reconnaissance stage of phishing or social engineering attacks. Social media can provide attackers the information they need to conduct further assaults, such as phishing and social engineering, or a platform to impersonate reputable individuals and brands.

Ali et al. (2018) discuss security threats in social networks, including malware, phishing, and cross-site scripting. They analyze user behavior and recommend solutions like privacy settings, personal information, antivirus, and third-party applications for improved security.

Abbasi et al. (2021) developed a phishing funnel model using support vector ordinal regression and cumulative link mixed models to represent user decisions across funnel stages, testing it with real-time data for 15 months.

Categories of Threats

In Acquisti et al. (2007) and Deliri & Albanese (2015), some threats are considered principal threats specifically to social networks. These threats are:

1. Privacy Related Threats
2. Variants of Traditional Network and Information Security Threats
3. Identity-related Threats
4. Social Threats

(i) **Privacy Related Threats**

Privacy-related threats on social networks refer to risks and vulnerabilities that can compromise users' personal information, online activities, and privacy while using social media platforms. Scammers exploit large data on social media accounts, posing risks due to data protection issues and privacy controls (Hetler, 2023). As gathered by Acquisti et al., (2007), Al-Charchafchi et al. (2020) and Hetler, 2023), here are some common privacy-related threats on social networks:

(i) ***Data mining for identity theft and impersonation***: Scammers do not need a great deal of information to steal someone's identity. They can start with publicly available information on social media to help target victims, which will result in digital dossier aggregation— collecting and compiling data from various sources to create a comprehensive profile of an individual's online activities, behaviors, and preference. Cybercriminals can gather personal information shared on social networks to impersonate users or commit identity theft. This can lead to financial fraud, reputation damage, or misuse of personal data.

(ii) ***Secondary Data collection and sharing***: Social networks often collect and store vast amounts of personal data from users, including profile information, posts, likes, and connections. This data can be used for targeted advertising, analytics, or shared with third parties without explicit user consent. Scammers can also gather the data that have already been collected by social networks for criminal purposes.

(iii) ***Privacy settings and controls***: Users may unknowingly expose their personal information or make their posts and profiles publicly accessible due to complex or confusing privacy settings on social networks. This can result in unintended disclosure of sensitive information.

(iv) ***Social engineering attacks***: Attackers can exploit information shared on social networks to launch targeted attacks, such as phishing scams, social engineering, or blackmail. They may use personal details to gain trust or manipulate users into revealing sensitive information.

(v) ***Cyberbullying and harassment***: Social networks can be breeding grounds for cyberbullying, harassment, and stalking. Users' personal information, posts, or photos can be misused to target and intimidate individuals, compromising their privacy and well-being.

(vi) ***Location tracking***: Some social networks collect and track users' location data, potentially revealing sensitive information about their whereabouts and daily routines. This can pose risks to personal safety and privacy.

(vii) ***Third-party app risks***: Users often grant access to their social media accounts to third-party apps or services. These apps may have inadequate security measures, leading to unauthorized access, data breaches, or misuse of personal information.

(viii) ***Targeted advertising and profiling***: Social networks track users' online activities, interests, and preferences to deliver personalized ads. This can infringe on users' privacy, manipulate their behavior, and result in invasive advertising practices.

(ix) ***Facial recognition***: Some social networks use facial recognition algorithms to identify and tag individuals in photos. Facial recognition technology on social networks can indeed pose security threats and raise concerns about privacy, consent, and the potential misuse of facial recognition data. Potential security threats associated with facial recognition on social networks include unauthorized access, identity theft, privacy invasion, data breaches, and surveillance and monitoring.

(x) ***Content-based Image Retrieval (CBIR)****:* Content-based image retrieval (CBIR) is a technique used to search and retrieve images from a database based on their visual content rather than relying on textual descriptions or metadata. It involves analyzing the visual features of an image, such as color, texture, shape, and spatial relationships, and comparing them to a query image to find similar or relevant images. Content-based image retrieval (CBIR) itself is not inherently a security threat on social networks. CBIR is a technique used for searching and retrieving images based on their visual content. However, there are potential security concerns related to the use of CBIR on social networks, which include: privacy, unauthorized access, and facial recognition.

(xi) ***Difficulty of Complete Account Deletion***: The difficulty of complete account deletion on social networks can indeed be considered a security issue, because it can result into data retention, which can be susceptible to unauthorized access or misuse, posing a security risk to users; data breaches, third-party data sharing, reidentification, and lack of control over personal information.

(ii) **Variants of Traditional Network and Information Security Threats**

These are various traditional risks and vulnerabilities that can compromise the confidentiality, integrity, and availability of data and systems within a network. They include:

(i) ***Malware***: This includes viruses, worms, Trojans, and other malicious software that can infect systems and networks, causing damage or stealing sensitive information.

(ii) ***Cross Site Scripting***: This is a security vulnerability that allows an attacker to inject malicious scripts into web pages viewed by other users. This occurs when a web application does not properly validate or sanitize user input before displaying it on a web page.

(iii) ***Spam***: This refers to unwanted or unsolicited messages, typically sent in bulk, through email, text messages, social media, or other communication channels. The term spam can also refer to unwanted advertisements, scams, or malicious content sent through these channels.

(iv) ***Aggregators***: Aggregators are platforms or websites that collect and display information or content from various sources in a centralized location. While aggregators can be beneficial in many contexts, they can also pose threats on social networks, through misinformation,

amplification of hate speech and extremism, manipulation of public opinion, intellectual property infringement, and more.

(v) ***Phishing***: Phishing attacks involve tricking users into revealing their personal or financial information by posing as a legitimate entity through emails, websites, or other communication channels.

(vi) ***Password attacks***: Password attacks involve attempting to gain unauthorized access to systems or accounts by guessing or cracking passwords through methods like brute force or dictionary attacks.

(vii) ***Social engineering***: Social engineering attacks exploit human psychology to manipulate individuals into revealing sensitive information or performing actions that compromise security.

(iii) **Identity-related Threats**

These threats include account takeover, catfishing, spear phishing using social network services and social-network-specific phishing, infiltration of networks leading to information leakage, profile-squatting and reputation slander through identity theft.

(iv) **Social Threats**

Social threats refer to various risks or dangers that can arise in social settings or interactions. These threats can negatively impact individuals, relationships, communities, or society as a whole. Social threats can manifest in different forms and contexts, including online platforms, offline interactions, and societal structures. Social threats on social networks include discrimination and prejudice, stalking, bullying, corporate espionage, hate speech, social manipulation and coercion, and public shaming.

5. Security and Privacy Requirements on Social Networks

Security and privacy requirements are very important on social networks, because inappropriate usage and unlawful disclosure of users' personal data might have unfavorable or detrimental effects on users' lives. They are crucial to protect user data and ensure a safe and trusted environment for users.

Zhang et al. (2010) categorizes privacy on social networks into three:

- **User's identity anonymity**: This is an important aspect of privacy and security on social networks. While some users may choose to use their real identities on social networks, others may prefer to remain anonymous for various reasons, such as personal safety, avoiding harassment, or expressing opinions without fear of repercussions. Tools used for user identity anonymity on social networks include pseudonyms and usernames, optional profile information, private messaging, content moderation, protection against doxing, and legal considerations.

- **User's personal space privacy**: This refers to the protection of a user's personal space, including their personal information, posts, photos, and activities, from unauthorized access or misuse by the social network. The visibility of a user's profile also varies across different social networks.
- **User's communication privacy**: This refers to the protection of a user's conversations and communications from unauthorized access, interception, or surveillance, through secure transmission, end-to-end encryption, protection against data mining, secure authorization, protection against spam and phishing, user reporting and moderation, and compliance with data protection regulations.

In summary, from the above categories of user's privacy requirements, a user's security and privacy needs can be grouped into two:

(i) ***Owner's Anonymity and Data Confidentiality***: The content of the private data that contains the identifying information of the data owner must not be discovered by unauthorized entities (i.e., those who are not authorized access to the private data). This component of data privacy necessitates access control because it implies data confidentiality and the owner's anonymity. Only the user may authorize others to access their personal data, and even then, access control must be as specific as possible to ensure that every piece of private data is kept under separate management.

(ii) ***Unlinkability Requirement***: The stored or transferred private data must appear random and leak no information that would allow unauthorized parties to link several private data files to the profile owner (Zhang et al., 2010).

By implementing these security and privacy requirements, social networks can enhance user trust, protect user data, and create a safer online environment for their users.

6. Handling Security and Privacy Threats on Social Networks

Social networks have become an integral part of our lives, allowing us to connect with friends, family, and even strangers from around the world. However, with the increasing popularity of social networks, there has been a rise in security and privacy threats. From the contributions of Raji et al. (2012) and Zhang et al. (2010), here are some steps you can take to handle these threats on social networks:

1. ***Use strong and unique passwords***: Create strong passwords that include a combination of letters, numbers, and special characters. Avoid using the same password for multiple social media accounts to prevent a domino effect if one account is compromised.

2. ***Enable two-factor authentication***: Two-factor authentication adds an extra layer of security to your social media accounts. It typically involves entering a verification code sent to your mobile device in addition to your password when logging in.
3. ***Be cautious about what you share***: Be mindful of the information you share on social media, especially personal details such as your address, phone number, or financial information. Limit the visibility of your posts to only trusted friends and avoid accepting friend requests from unknown individuals.
4. ***Regularly review privacy settings***: Social media platforms often update their privacy settings, so it's essential to review and adjust your settings regularly. Make sure you understand who can see your posts, photos, and personal information and adjust the settings accordingly.
5. ***Beware of phishing attempts***: Be cautious of suspicious messages or links you receive on social media. Phishing attempts can trick you into revealing your login credentials or personal information. Avoid clicking on suspicious links and always verify the authenticity of messages before responding.
6. ***Keep your devices and software up to date***: Regularly update your devices, including smartphones, tablets, and computers, with the latest security patches and software updates. These updates often include security enhancements that protect against known vulnerabilities.
7. ***Use reputable antivirus software***: Install reputable antivirus software on your devices to detect and remove malware or viruses that could compromise your social media accounts.
8. ***Be skeptical of third-party apps***: Be cautious when granting permissions to third-party apps that request access to your social media accounts. Only authorize apps from trusted sources and review the permissions they require.
9. ***Report and block suspicious accounts***: If you encounter suspicious or abusive accounts on social media, report them to the platform's support team. Blocking these accounts will prevent them from interacting with you and accessing your information.
10. ***Educate yourself and others***: Stay informed about the latest security and privacy threats on social media. Educate yourself and others in your network about best practices for staying safe online.

Remember, maintaining security and privacy on social networks is an ongoing effort. By following these steps and staying vigilant, you can minimize the risks and enjoy a safer online experience.

7. Emerging Social Network Security Threats and Challenges

In an ENISA publication by Mattioli et al. (2023), the study identified, ranked, and collected information on ten future cybersecurity threats and challenges. The highlighted threats are shown in Figure 1 below. The study proposes that "in 8 years, many of today's threats will remain pressing but will have shifted in character – increased dependencies and the democratization and development of new technologies add complexity to our understanding of threats".

Figure 1: Emerging Cybersecurity Threats for 2030

***Source**: ENISA Foresight Exercise 2022*

The proposed threats, as contained in the ENISA Foresight Exercise 2020, are:

1. Supply chain compromise of software dependencies
2. Advanced disinformation campaigns
3. Rise of digital surveillance authoritarianism / loss of privacy
4. Human error and exploited legacy systems within cyber-physical ecosystems
5. Targeted attacks (e.g. Ransomware) enhanced by smart device data
6. Lack of analysis and control of space-based infrastructure and objects
7. Rise of advanced hybrid threats
8. Skill shortages
9. Cross-border ICT service providers as a single point of failure
10. Abuse of Artificial Intelligence.

Each of the above emerging threats is described in APPENDIX I.

Based on current trends and patterns, the following potential emerging cyber security threats and challenges may require attention and action.

1. ***Deepfake technology***: Deepfakes are manipulated or fabricated audio and video content that appears to be real, often used to deceive and manipulate individuals. This technology can be used to spread misinformation, defame individuals, or manipulate public opinion.
2. ***Artificial Intelligence (AI) and Machine Learning (ML) Attacks***: As AI and ML continue to advance, cyber criminals may use these technologies to launch more sophisticated and targeted attacks. This could include using AI to automate attacks, create more convincing phishing emails, or even create deepfakes to manipulate individuals or organizations.
3. ***Internet of Things (IoT) Security***: The proliferation of IoT devices in homes, businesses, and public spaces can create vulnerabilities that hackers can exploit. As more devices become interconnected, it may become easier for hackers to gain access to sensitive data or even take control of critical systems.
4. ***Quantum Computing Threats***: Quantum computing has the potential to break current encryption methods, which could make sensitive data vulnerable to theft or manipulation. As quantum computing becomes more advanced, it may become easier for cyber criminals to exploit this weakness.
5. ***Nation-State Cyber Attacks***: Nation-states may continue to use cyber-attacks as a means of espionage or even warfare. These attacks can be difficult to detect and defend against, and may have serious consequences for national security and global stability.
6. ***Cybersecurity Workforce Shortage***: As the demand for cybersecurity professionals continues to grow, there may be a shortage of qualified individuals to fill these roles. This could leave organizations vulnerable to cyber-attacks and make it more difficult to respond to emerging threats.
7. ***Phishing and social engineering attacks***: Cybercriminals are increasingly using social networks as a platform to launch phishing attacks, tricking users into revealing sensitive information or downloading malicious software. Social engineering techniques, such as impersonation or exploiting personal relationships, are employed to manipulate individuals into taking actions that compromise their security.

These potential threats and challenges highlight the need for continued investment in cybersecurity research, education, and infrastructure. It is important for individuals, organizations, and governments to stay vigilant and proactive in addressing emerging cyber security threats.

8. New Paradigm for Security on Social Networks

Cybersecurity requires continuous anticipation of threats to avoid and mitigate risks, but these measures should not compromise necessary controls like education, awareness, and patching (Mattioli et al., 2023). To address the emerging security threats, social networks must invest in robust security measures, implement strict privacy controls, and enhance user education and awareness. Users should also take proactive steps to protect themselves, such as using strong and unique passwords, enabling two-factor authentication, being cautious of suspicious links or messages, and regularly reviewing and updating privacy settings (Alqatawna et al., 2017).

Information Identifiability and Linkability

The use of personal information in social networks raises privacy concerns and security issues. Online social networks pose a challenge due to increased risk and user lack of awareness. Protecting information identifiability and linkability is difficult, as even sites that don't disclose users' personal information can provide enough data to identify and link profiles. Hosting servers for social networking sites, the network itself, and other parties who might abuse or misuse such sensitive and important information are examples of potential recipients of such personally identifiable information (Ali et al., 2018).

Interpersonal Relationships and Flexibility

A new paradigm for security in online social networks is needed to address interpersonal relationships and flexibility. An individual could, for example, share their private photo album with relatives but not with coworkers. Users of social networking sites can choose which other users to map to a limited profile they create. Current security mechanisms have limited expressiveness, especially in dynamic networks. New security mechanisms based on risk, trust, and social metrics are becoming more compelling (Ali et al., 2018).

Social networks' security and privacy requirements are not fully understood, but they differ from classic security and privacy requirements due to user-centric concerns and multiple user-specified policies. Experience from various domains and technologies is needed. Therefore, we must bring extensive security experience from various domains and technologies to this field, along with a comprehensive understanding of social networks. (Ahn et al., 2011; Ali et al., 2018).

As technology continues to advance, it is crucial for individuals, organizations, and policymakers to remain vigilant and adapt to the evolving landscape of security threats on social networks. By working together, we can create a safer and more secure online environment for everyone.

9. Conclusion

The issue of security and privacy on social networks is a complex and pressing concern in today's digital age. With the increasing reliance on social media platforms for communication, networking, and information sharing, individuals are exposed to various risks and threats that can compromise their personal data, well-being, and even their safety. The rapid growth of social networks has brought about numerous benefits, such as facilitating global connectivity and fostering communities. However, it has also created opportunities for malicious actors to exploit vulnerabilities and engage in harmful activities, such as cyberbullying, identity theft, and online scams.

To address these challenges, it is crucial for social network platforms, governments, and individuals to work together to enhance security measures and promote privacy protection. Social media companies should invest in robust security infrastructure, including encryption, authentication mechanisms, and proactive monitoring systems to detect and prevent potential threats. Additionally, they should provide users with transparent privacy settings and clear guidelines on data collection, usage, and sharing. Governments play a vital role in establishing and enforcing regulations that protect users' privacy rights and hold social network platforms accountable for any breaches or mishandling of personal data. Public awareness campaigns and educational initiatives can also empower individuals to make informed decisions about their online presence and take steps to safeguard their privacy.

Ultimately, the responsibility lies with each individual to actively manage their online presence and adopt safe practices while using social networks. This includes being cautious about sharing personal information, regularly updating privacy settings, and being mindful of the content they engage with and share. Through collective effort towards addressing the issues of security and privacy on social networks, we can create a safer and more trustworthy digital environment that fosters positive interactions, protects personal data, and respects individuals' rights to privacy and security.

References

Acquisti, A., Carrara, E., Stutzman, F., Callas, J., Schimmer, K., Nadjm, M., Gorge, M., Ellison, N., King, P., Gross, R., & Golder, S. (2007). Security Issues and Recommendations for Online Social Networks. In *European Union Agency for Cybersecurity (ENISA) Position Paper* (Vol. 1, Issue 1). https://www.enisa.europa.eu/publications/archive/security-issues-and-recommendations-for-online-social-networks/

Ahn, G. J., Shehab, M., & Squicciarini, A. (2011). Security and Privacy in Social Networks. *IEEE Internet Computing*, *15*(03), 10–12. https://doi.org/10.1109/MIC.2011.66

Al-Charchafchi, A., Manickam, S., & Alqattan, Z. N. M. (2020). Threats Against Information Privacy and Security in Social Networks: A Review. *Communications in Computer and Information Science*, *1132 CCIS*, 358–372. https://doi.org/10.1007/978-981-15-2693-0_26

Ali, S., Islam, N., Rauf, A., Din, I. U., Guizani, M., & Rodrigues, J. J. P. C. (2018). Privacy and Security Issues in Online Social Networks. *Future Internet 2018, Vol. 10, Page 114*, *10*(12), 114. https://doi.org/10.3390/FI10120114

Alqatawna, J., Madain, A., Al-Zoubi, A. M., & Al-Sayyed, R. (2017). Online social networks security: Threats, attacks, and future directions. *Social Media Shaping E-Publishing and Academia*, 121–132. https://doi.org/10.1007/978-3-319-55354-2_10

Ayodeji, O. G., & Kumar, V. (2019). Social media analytics: A tool for the success of online retail industry. *International Journal of Services Operations and Informatics*, *10*(1), 79–95. https://doi.org/10.1504/IJSOI.2019.100630

Boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://doi.org/10.1111/J.1083-6101.2007.00393.X

Chen, H., & Yang, C. C. (2008). *Intelligence and Security Informatics*. *135*. https://doi.org/10.1007/978-3-540-69209-6

Deliri, S., & Albanese, M. (2015). *Security and Privacy Issues in Social Networks*. 195–209. https://doi.org/10.1007/978-3-319-20062-0_10

Fong, P. W. L., Anwar, M., & Zhao, Z. (2009). A privacy preservation model for facebook-style social network systems. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5789 LNCS*, 303–320. https://doi.org/10.1007/978-3-642-04444-1_19/COVER

Hetler, A. (2023). *6 common social media privacy issues*. WhatIs.Com. https://www.techtarget.com/whatis/feature/6-common-social-media-privacy-issues

Joshi, P., & Kuo, C. C. J. (2011). Security and privacy in online social networks: A survey. *Proceedings - IEEE International Conference on Multimedia and Expo*. https://doi.org/10.1109/ICME.2011.6012166

Kenton, W. (2023, April 24). *What Is Social Networking?* Investopedia. https://www.investopedia.com/terms/s/social-networking.asp

Mattioli, R., Malatras, A., Hunter, E. N., Penso, M. G. B., Bertram, D., & Neubert, I. (2023). Identifying Emerging Cyber Security Threats and Challenges for 2030. In *European Union Agency for Cybersecurity (ENISA)*. https://doi.org/10.2824/117542

Naseer, H. (2023, February 6). *Understanding and Exploring Social Media Features*. Sprout Social. https://sproutsocial.com/insights/social-media-features/

Patil, V. T., & Shyamasundar, R. K. (2017). Undoing of privacy policies on facebook. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10359 LNCS*, 239–255. https://doi.org/10.1007/978-3-319-61176-1_13

Raji, F., Miri, A., & Davarpanah Jazi, M. (2012). Preserving privacy in online social networks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6888 LNCS*, 1–13. https://doi.org/10.1007/978-3-642-27901-0_1

Zhang, C., Sun, J., Zhu, X., & Fang, Y. (2010). Privacy and security for online social networks: Challenges and opportunities. *IEEE Network*, *24*(4), 13–18. https://doi.org/10.1109/MNET.2010.5510913

APPENDIX I

EMERGING CYBERSECURITY THREATS FOR 2030

TOP 10 EMERGING CYBERSECURITY THREATS FOR 2030
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
THREATS
2030
1
Supply chain compromise of software dependencies
More integrated components and services from third party suppliers and partners could lead to novel and unforeseen vulnerabilities with compromises on the supplier and customer side.
2
Advanced disinformation campaigns
FAKE
Deepfake attacks can manipulate communities for (geo)political reasons and for monetary gain.
3
Rise of digital surveillance authoritarianism/ loss of privacy
Facial recognition, digital surveillance on internet platforms or digital identities data stores may become a target for criminal groups
4
Human error and exploited legacy systems within cyber-physical ecosystems
The fast adoption of IoT, the need to retrofit legacy systems and the ongoing skill shortage could lead to a lack of knowledge, training and understanding of the cyber-physical ecosystem, which can lead to security issues.
5
Targeted attacks enhanced by smart device data
Through data obtained from internet-connected smart devices, attackers can access information for tailored and more sophisticated attacks.
6
Lack of analysis and control of space-based infrastructure and objects
Due to the intersections between private and public infrastructure in space, the security of these new infrastructures and technologies need to be investigated as a lack of understanding, analysis and control of space-based infrastructure can make it vulnerable to attacks and outages.
7
Rise of advanced hybrid threats
Physical or offline attacks are evolving and becoming often combined with cyberattacks due to the increase of smart devices, cloud usage, online identities and social platforms.
8
Skill shortage
Lack of capacities and competencies could see cybercriminal groups target organisations with the largest skills gap and the least maturity.
9
Cross border ICT service providers as a single point of failure
ICT sector connecting critical services such as transport, electric grids and industry that provide services across borders are likely be to targeted by techniques such as backdoors, physical manipulation, and denials of service and weaponised during a future potential conflict.
10
Artificial Intelligence Abuse
AI
Manipulation of AI algorithms and training data can be used to enhance nefarious activities such as the creation of disinformation and fake content, bias exploitation, collecting biometrics and other sensitive data, military robots and data poisoning.
Source: ENISA Foresight excercise 2022
Reproduction is authorised, provided the source is acknowledged
enisa